Comparative Analysis of Various Biometric Techniques for Database Security

Harpreet Saini[1], Kanwal Garg[2]

[1]Research Scholar, M. Tech Department of Computer Science and Application
Kurukshetra University Kurukshetra, India
hs7004@gmail.com

[2]Assistant Professor, Department of Computer Science and Application
Kurukshetra University Kurukshetra, India
gargkanwal@yahoo.co

Abstract: ***The premise of this paper is to analyze the various biometric techniques. This paper provides an overview of different biometric technique with some advantages and disadvantages. The comparison criteria presented in this paper is limited to acceptance, cost, accuracy, performance and cost. Author will try to find out which technique is more reliable and secure.***

Keywords: Authentication, Biometric, Database

1. Introduction

Biometric recognition refers to the use of different physiological characteristics like fingerprint recognition, face recognition, retina recognition, hand geometry recognition, iris recognition etc. and behavioural characteristics such as voice recognition, gait recognition, signature recognition etc. called biometric identifiers or biometrics. For authentication purpose these features are used in computer based security system. The identification of a person is becoming very important as the ID cards, username, secret password and PIN which are used for the personal identification. The ID can be stolen by someone and the PIN Number can be forgotten but the biometric techniques overcome all these problems. The biometric system offers various advantages over traditional authentication system. The problem of information security gives protection of information ensuring only authorized users are able to access the information. They are required the person being authenticated to be present at the point of authentication [8].Thus biometric methods are most secure methods. A stable identification system is a critical component in several applications that contribute their services correctly to genuine users. Examples of such applications consist of physical access control to a secure facility, e-commerce, access to computer networks, attendance mark etc. Traditional methods of building a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms. As a result, they are not sufficient for identity verification in the modern day world. As it is well known that security is very important aspect in every field, in the same it is important in the field of database also. The author tries to find the solution of database issues using biometric techniques.

The presented paper comprises of seven sections. The first section elaborates the introductory part and the second one is About literature survey. The third one is explaining the modes of biometric techniques which are further subdivided into two parts: enrolment and authentication process. The fourth section is discussing about the techniques of biometric and fifth one is describing the resultant table of comparison of various biometric techniques. The last two sections represent the conclusion and references.

2. Review of Literature

In this section the author has discussed some research papers which had been previously undertaken in the field of biometric system:

Mary Lourde R had elaborated about the issue of selection of an optimal algorithm for matching the fingerprint in order to design a system that matches required specifications in performance and accuracy. Srinivasulu Asadi has discussed the different face recognition techniques by considering different test samples. Khattab M. Ali has implemented the iris recognition algorithm using histogram equalization and wavelet techniques. Tiwalade O.Majekodunmi, Francis E.idachaba has explained in his review paper about the four techniques i.e. fingerprint recognition, face recognition, iris recognition and speaker recognition and there mode of operation of each technique with their advantages and disadvantages.

3. Modes of Biometric System

There are two operational modes in biometric authentication system as shown in fig.1. The first one is the enrolment process and the second one is authentication process. The authentication process is further divided into two categories, the verification process and the identification process. Further the identification is divided into two categories i.e. positive identification and negative identification. In the upcoming section these modes are explored in detail.

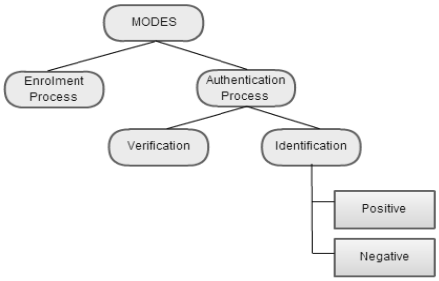

Figure 1. Modes of Biometric System

3.1 Enrolment Process

When the first time an individual uses a biometric system it is called as enrolment. During this, biometric information from an individual is captured and stored. Then biometric information is detected and compared with the information stored information at the time of enrolment. The sensor is the interface between the real world and the system; it has to acquire all the essential data. The second block performs all the necessary pre-processing i.e. it has to remove old object from the sensor to improve the input like removing background noise. In the third block significant features are extracted. This step is an important step because the correct features need to be extracted in the best way. To create a template an image with particular properties is used. A template is a construction of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size [2].

3.2 Authentication Process

The basic block diagram of a biometric can be in the following two modes, either in verification mode or in identification mode.

In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify that individual is the person they claim to be. In this firstly the reference models for all the users are generated and stored in the model database than some samples are matched with reference models to generate the genuine and impostor scores.

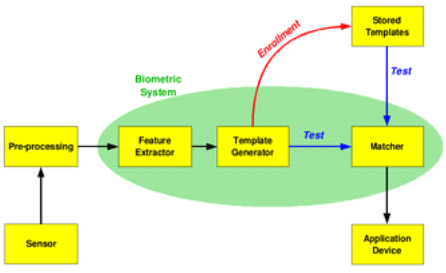

Figure 2. Enrolment Process in Biometric
Source: http://en.wikipedia.org/wiki/Biometrics

At last testing is done. This process may use a smart card, username or ID number (e.g. PIN) to suggest which template should be used for comparison. The common use of verification mode is 'Positive recognition' where the aim is to prevent multiple people from using same identity.

In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish (authorize, found) the identity of an unknown individual. The system will accomplish in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' or for 'negative recognition' of the person. Positive identification explains “Who am I?” although the response can be a name or it could be an employee ID or another unique identifier. A typical positive identification system would be a prison release program where users do not enter an ID number or use a card, but simply look at an iris capture device) and are identified from a convict database. Negative identification systems also search databases in the same fashion by comparing one template against many, but are designed to conform that a person is not present in a database. This prevents people from entering twice in a system, and is often used in large-scale public benefits programs in which users enter multiple times to gain benefits under different names.

4. Techniques

The purpose of biometrics system is to uniquely identify or verify an individual through the characteristics of the human body. There are several techniques of biometric which is mainly divided into two categories i.e. physiological characteristics and behavioural characteristics as described below through a flow chart. The physiological characteristics which are discussed in this paper are fingerprint, iris, retina, face and hand geometry whereas the behavioural characteristics which are discussed are voice and signature characteristics.

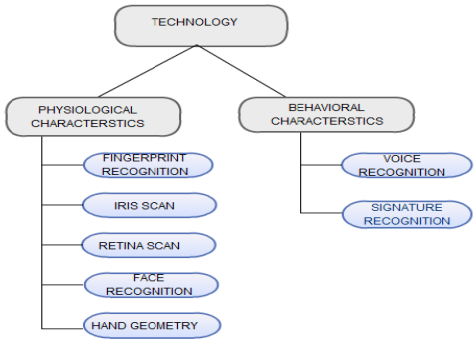

Figure 2 Types of Biometric Techniques

4.1 Fingerprint Recognition

Fingerprinting is one of the oldest and the most extensive means of identification in use today. An individual’s fingerprints are defined by a composite combination of patterns: lines, arches, loops, and whorls. In this technique the image of a person's fingertips is taken (either using ink or a digital scan) and records its characteristics. Whorls, arches, and loops are recorded along with the patterns of

ridges, furrows, and minutiae and this information may then be processed or stored as an image to be compared with other fingerprint records. In this technique, the user attached to a presses his finger gently against a small reader surface (optical or silicon) at the time of verification for less than 5 seconds and the size of reader is about 2 inch square. The reader is computer and takes the information from the scanner and sends it to the database and then it is compared to the information within. There is a database of fingerprint technique known as Automated Fingerprint Identification System (AFIS) which is taken and stored in the United States as other countries like Canada and the United Kingdom. Each person's fingerprints are unique. This technique is most important as it has high reliability, accuracy and it is highly distinctive but due to dry skin, poor environment or injury this technique might not be useful. Modern fingerprint techniques supported by computer and laser technology have fast the process of searching for matches and provided a large database of comparative specimens.

4.2 Iris recognition

Iris scans determine the features that exist in the coloured tissue surrounding the pupil which has more than 200 points that can be used for comparison. In this technique, the user places him so that he can see the reflection of his own eye on the device. Unlike the retinal scanner, the iris scanner can be placed 12 to 18 inches apart from the person who is using it. The Verification time is generally less than 5 seconds as the user only need to look into the device for a couple of moments. In comparison this is stored version of the user's iris pattern stored on the user's identification card or in a central database. This database is a collection of images which contain iris region of the eye and the images are stored by sensor that operates in visible spectrum. If match occurs then user is authenticated. Iris recognition is fast, non-invasive. It may be better than fingerprints in terms of FAR. The iris technique is more unique than the fingerprint but less than the retina. This technology is extremely effective with high accuracy as it uses more than 240 points of references for a match but as compare to it, fingerprint technique uses only 60 points. This technique does not involve any touch as fingerprint involves. They are considered to be more good and secure but it is very expensive and need lot of memory to store the data.

4.3 Retinal scanning

Retinal scanning examines the layer of blood vessels at the back of the eye. Scanning involves a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. In this technique, the user looks through a small opening in the device at a small green light and requires the user to remove glasses, place their eye close to the device. After doing this the user has to focus on a certain point for few seconds during that time period the device will verify his identity. Then this profile is compared to a profile stored on the central database. If match occurs then user is authenticated. There are mainly two types of databases that contains the colour images of the retina acquired using a retinograph with or without pupil dilation during routine clinical examination. This process takes about 10 to 15 seconds in total. Retinal scanning is considered to be invasive whereas iris is not because there is no way to replicate a retina and size of template is small as compared to iris. A retina from a dead person would degrade too fast to be useful so no extra cautions have been taken with retinal scans to be sure the user is a living human being.

4.4 Facial Recognition

This technique analyses the characteristics of a person's face images using a digital video camera. It measures the complete facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are saved in the database and used as a comparison when a user stands before the camera. This technique is now used in verification systems only with a good deal of success. In this technique, the user faces the camera by standing about two feet away from it. The user's face is located by the system and then match is performed against the claimed identity or the facial database. The Facial Recognition Technology Database (FERET) is a database whose main mission was to develop automatic face recognition capabilities that could be employed to provide security. It is possible that the user may require moving and reattempting the verification based on his facial position and its verification time is less than 5seconds. It is a cheap technology, non-intrusive and has high acceptance but can be fooled by the identical twins and also face changes over time.

4.5 Voice Recognition

Voice recognition systems use characteristics of the voice like pitch, tone, frequency, etc. This technique mainly focuses on the differences which are resulting from the shape of vocal tracts and learned speaking habits.

In this technique, the user speaks a specific word into a microphone attached to the system. Software examines his or her voice and extracts significant quantity on roughly twenty parameters like pitch, speech, energy density, waveforms, etc. This live profile is correlated against a profile stored on a central database where whole data is stored. If a good match occurs then user is authenticated. Voice recognition is one of the simplest technique as it is easy to use, non-intrusive and cheap technology but due to poor environment, cold it can create problem, also has low accuracy. The changes in a person's voice are slightly due to physical attributes, but mostly due to behaviour patterns. Vocal cords vibrate at about 80 times per second for men and 400 times per second for women. These vibrations are modified by the size of the jaw opening, by tongue, lip shape and positions which are some factors that make each person's voice unique.

4.6 Signature Recognition

The least effective biometric authenticator was Signature recognition. The text involved in a signature is continuous and regular in nature. The user signs on a tablet or on the paper that placed over a sensor tablet. The device records the signature of the user and compares it to its database and the verification takes about 5 seconds. The technology is

promoted by low-cost, writing tablet; this significantly improves the cost efficiency of this biometric without suffering an adequate loss in the ability of the biometric to perform at high accuracy levels. This technology is cheap, non-intrusive, has low cost, high user acceptance and require low training but it changes over time and has low distinctiveness**.**

4.7 Hand Geometry

In this technique, the user places the palm of his hand on a metal surface, positions his or her fingers according to a set of pins on the device and waits approximately for 1.2 seconds. The hand is properly aligned so that the device can read the hand attributes. Then the database is checked by the device where whole information of the user is stored for verification of the user. This process usually takes less than 5 seconds. Current hand geometry scanners do not have any way to find whether a hand is living or not and hence can be fooled by a fake hand if pressure is applied to the plate correctly. The memory space needed to store the template is typically very small. This technique involves the measurement and analysis of the shape of user's hand. It is a fairly simple procedure and accurate. Also it is unaffected by skin condition. Though it requires special hardware to use, it can be easily integrated into other devices. Unlike fingerprints, the human hand is not unique. Individual hand features are not clear enough for identification. However, it is possible to construct a method by combining various individual features and measurements of fingers and hands for verification purposes. This technique becomes popular in small organizations because of its low cost and high performance.

Various competing technology solutions exist to solve the problem of human identification and the number of competing technologies in the field of automated ID systems has increased extremely. However fingerprint remains with hand geometry technique, most widely used technology. Fingerprint technique is more appropriate in comparison to hand geometry as the human hand is not unique. Individual hand features are not clear enough for identification. The signature technique is least effective as signature of person can vary with time. Iris scan may be better than fingerprint in term of false accept rate and also more unique than the fingerprint but less than the retina. In above table the comparison is done between various techniques and finds the best one.

5. Resultant Table

Table1. Comparative Analysis of Various Biometric Techniques

	Acceptance	Accuracy	Uniqueness	Cost	Performance	FAR	FRR
Finger Print	M	H	H	M	H	1 to 10 in 100,000 (.001-.01%)	3 to 7 in 100 (3-7%)
Iris Scan	M	H	H	H	H	>=.001%	in 100 (2-10%)
Retina	M	H	H	H	H	NA	NA
Facial	M	M	L	M	L	100 to 1000 in 100,000 (.1-1%)	10 to 20 in 100 (10-20%)
Voice	H	M	L	M	L	2000 to 5000 in 100,000(2-5%)	10 to 20 in 100 (10-20%)
Signature	V H	L	L	M	L	2-5%	10 to 20 in 100 (10-20%)
Hand geometry	H	M	M	L	M	0 in 1000 (1-2%)	1 to 2 in 100 (1-2%)

As given above compares some of the biometric techniques keeping in view about accuracy, false accept rate and reject rate, uniqueness, performance, acceptability, etc.

6. Conclusion

In this paper the main focus is given on comparing various techniques of biometric according to accuracy, cost, false accept rate and reject rate etc. as explained in the above table. Therefore from keeping in view the above explained techniques with the comparison table the author has concluded that while the iris technique provides to be the most secure, voice and face biometric techniques had the highest level of user acceptance, the fingerprint technique is the fast and accurate biometric technique for more reliable and secure system and offered the best overall solution.

References

[1] Alessandra Lumini and Loris Nanni "when Fingerprint are Combined with Iris- A case Study: FVC2004 and CASIA" published in the proceeding of Network Security, Vol.4, No.1, PP.27-34, Jan. 2007.

[2] Mary Loured R and Dushyant Khosla "Fingerprint Identification in Biometric Security System" published in the proceeding of international journal of computer and electrical engineering, Vol. 2, No. 5, October, 2010, ISSN 1793-8163.

[3] Srinivasulu Asadi, Dr. Ch. D. V. Subba Rao, V. Saikrishna "A Comparative Study of Face Recognition with Principal Component Analysis and Cross – Correlation Techniques" published in the proceeding of international journal of computer application, Vol. 10, NO-8, November 2010, ISSN 0975-8887.

[4] Khattab M. Ali Alheeti "Biometric Iris Recognition Based on Hybrid Technique" published in the proceeding of international journal of soft computing (IJSC), Vol.2, No.4, November 2011.

[5] Arpita Gopal and Chandrani Singh "e-World: Emerging Trends in Information Technology" published in the proceeding of Excel Publication, New Delhi (2009).

[6] K P Tripathi "A comparative study of biometric technologies with reference to human interface" published in the proceeding of international journal of

computer application, Vol 14-No.5, January 2011, ISSN 0975-8887.

[7] Chanderkant Verma "Improving Biometric security Using Cryptography" published in the proceeding of international journal of advance research in computer engineering, ISSN 0974,Vol-1,PP 33-38, Jan-dec 2007.

[8] Chanderkant Verma "Soft Biometric: An Asset for Personal Recognition" published in the proceeding of international journal of computer science & communication technologies, ISSN 0974-3375,Vol-1,PP. 160-163, Jan 2009.

[9] Tiwalade O.Majekodunmi, Francis E.Idachaba "A Review Of The Fingerprint Recognition, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technology" published in the proceeding of world congress on engineering 2011, Vol.2, WCE 2011,July 6-8,2011, London, U.K.

[10] Mr. Sanjay Kumar and Dr. Ekta Walia "Analysis Of Various Biometric Techniques" published in the proceeding of international journal of computer science and information technology, Vol.2(4),2011,1595-1597, ISSN:0975-9646.

Authors Profile

Miss. Harpreet Saini received the B. Tech degree in computer science and engineering from Kurukshetra University in 2011. She is now pursuing M. Tech in computer science from department of computer science and application at the Kurukshetra University, Haryana. This author has published one review paper at national level. Her research interest includes database security and the **B**iometric.

Dr Kanwal Garg presently working as Assistant Professor in Department Of Computer Science And Application, Kurukshetra University Kurukshetra. Apart from district topper in senior secondary examination and Kurukshetra University topper in under graduation examination, he had completed his post graduation & doctorate from GJU S&T, Hisar under the faculty of Engineering and Technology. Owe the credit of more than 45 research papers published in international & national journals, conference & seminar. He attended 12 workshops/faculty Development Programme/winter/summer school and 01 Orientation Programme to enhance his curriculum. His area of expertise is Data Bases, Data Mining, & warehousing. Approximately 11 year of experience in teaching industry and administration. During this tenure he is actively involved in organizing co-curricular & social activities.